DOCUMENT RESUME

ED 140 815 IR 004 906

AUTHOR	Wood, Helen M.
TITLE	The Use of Passwords for Controlled Access to Computer Resources. Computer Science & Technology.
INSTITUTION	National Bureau of Standards (DOC), Washington, D.C. Inst. for Computer Sciences and Technology.
REPORT NO	NBS-SP-500-9
PUB DATE	May 77
NOTE	60p.
AVAILABLE FROM	Superintendent of Documents, U.S. Government Printing Office, Washington, D.C. 20402 (C13.10:500-9, Stock No. 003-003-01770-1, $2.00)
EDRS PRICE	MF-$0.83 HC-$3.50 Plus Postage.
DESCRIPTORS	Annotated Bibliographies; Computer Science; *Dial Access Information Systems; *Identification; Man Machine Systems; Networks; *On Line Systems; *Security
IDENTIFIERS	Passwords

ABSTRACT

This paper considers the generation of passwords and their effective application to the problem of controlling access to computer resources. After describing the need for and uses of passwords, password schemes are categorized according to selection technique, lifetime, physical characteristics, and information content. Password protection, both in storage and transmission, is dealt with in the next section, followed by brief sections on current implementations and cost considerations. A glossary and an annotated bibliography of all referenced material are included. (Author)

****
* Documents acquired by ERIC include many informal unpublished *
* materials not available from other sources. ERIC makes every effort *
* to obtain the best copy available. Nevertheless, items of marginal *
* reproducibility are often encountered and this affects the quality *
* of the microfiche and hardcopy reproductions ERIC makes available *
* via the ERIC Document Reproduction Service (EDRS). EDRS is not *
* responsible for the quality of the original document. Reproductions *
* supplied by EDRS are the best that can be made from the original. *
****

ED140815

COMPUTER SCIENCE & TECHNOLOGY:

The Use of Passwords for Controlled Access to Computer Resources

U.S. DEPARTMENT OF HEALTH, EDUCATION & WELFARE
NATIONAL INSTITUTE OF EDUCATION

THIS DOCUMENT HAS BEEN REPRODUCED EXACTLY AS RECEIVED FROM THE PERSON OR ORGANIZATION ORIGINATING IT. POINTS OF VIEW OR OPINIONS STATED DO NOT NECESSARILY REPRESENT OFFICIAL NATIONAL INSTITUTE OF EDUCATION POSITION OR POLICY.

Helen M. Wood

Institute for Computer Sciences and Technology
National Bureau of Standards
Washington, D.C. 20234

IR004906

U.S. DEPARTMENT OF COMMERCE, Juanita M. Kreps, Secretary

Dr. Betsy Ancker-Johnson, Assistant Secretary for Science and Technology

NATIONAL BUREAU OF STANDARDS, Ernest Ambler, Acting Director

Issued May 1977

Reports on Computer Science and Technology

The National Bureau of Standards has a special responsibility within the Federal Government for computer science and technology activities. The programs of the NBS Institute for Computer Sciences and Technology are designed to provide ADP standards, guidelines, and technical advisory services to improve the effectiveness of computer utilization in the Federal sector, and to perform appropriate research and development efforts as foundation for such activities and programs. This publication series will report these NBS efforts to the Federal computer community as well as to interested specialists in the academic and private sectors. Those wishing to receive notices of publications in this series should complete and return the form at the end of this publication.

National Bureau of Standards Special Publication 500-9

Nat. Bur. Stand. (U.S.), Spec. Publ. 500-9, 59 pages (May 1977)
CODEN: XNBSAV

Library of Congress Cataloging in Publication Data

Wood, Helen M.
The use of passwords for controlled access to computer resources.

(Computer science & technology) (NBS special publication ; 500-9)
Supt. of Docs. no.: C13.10:500-9
1. Computers—Access control—Passwords.
I. Title. II. Series. III. Series: United States. National Bureau of Standards. Special publication ; 500-9.
QC100.U57 no. 500-9 [QA76.9.A25] 602'.1s [001.6'4] 77-5558

U.S. GOVERNMENT PRINTING OFFICE
WASHINGTON: 1977

For sale by the Superintendent of Documents, U.S. Government Printing Office
Washington, D.C. 20402 - Price $2.

Stock Number 003-003-01770-1

ACKNOWLEDGEMENTS

Although much of the material in this report can be found in the open literature, a portion of it was obtained from correspondence and conversations. Among the individuals contributing information were James Anderson (James P. Anderson and Co.), Robert Jacobson (Chemical Bank), M. Blake Greenlee (Citibank), Maj. Roger Schell (Hanscom AFB), Robert Courtney (IBM Corporation), and Lt. Joseph Nichols (Air Force Data Services Center).

As a member of the Federal Information Processing Standards Task Group 15 (Computer Security), the author received numerous suggestions and ideas from other members of the group. These include Dennis K. Branstad (National Bureau of Standards), Francis R. Cappelletti (Defense Investigative Service), and several others, identified above. This help is gratefully acknowledged.

This study comprised a portion of the author's thesis research. The committee consisted of Dr. Nathaniel Macon, Chairperson (American University); Dr. Stanley Winkler (IBM Corporation and the American University); and Dr. Walter Jacobs (American University).

TABLE OF CONTENTS

INTRODUCTION 1

AUTHENTICATION 4

USES OF PASSWORDS. 6

PASSWORD SCHEMES 8

- Password Selection 8
- Password Lifetime. 10
- Physical Characteristics 13
- Information Content. 16
- Handshaking Schemes. 17

PASSWORD PROTECTION. 19

- Initial Distribution 19
- Password Storage 20
- Password Transmission. 23

CURRENT IMPLEMENTATIONS. 26

COST CONSIDERATIONS 28

CONCLUSIONS 30

GLOSSARY 33

SELECTED BIBLIOGRAPHY 38

THE USE OF PASSWORDS FOR CONTROLLED ACCESS TO COMPUTER RESOURCES *

Helen M. Wood

ABSTRACT

This report considers the generation of passwords and their effective application to the problem of controlling access to computer resources. After describing the need for and uses of passwords, password schemes are categorized according to selection technique, lifetime, physical characteristics, and information content. Password protection, both in storage and transmission, is dealt with in the next section, followed by brief sections on current implementations and cost considerations. A glossary and an annotated bibliography of all referenced material are included.

KEYWORDS: Computer networking; computer security; controlled access; identification; passwords; personal authentication.

INTRODUCTION

With the growth of timesharing and other forms of computer networking, the use of remotely accessed computers has become widespread. However, with this ease of access have come increased operational risks. The physical security of automatic data processing systems has been covered elsewhere in numerous papers and reports. (For guidelines on ADP physical security and risk management see [FIPS 31].) This report is concerned solely with the problem of authenticating an individual's claimed identity in an on-line computing environment.

Systems without adequate access controls are more vulnerable to threats including theft, fraud, and vandalism. Potential losses range from unauthorized use of computing time to the unauthorzed access, modification, or destruction of confidential data. Perpetrators of such abuse may be otherwise honest individuals wishing to play a few computer

---

* Certain commercial products are identified in this report in order to adequately specify the procedure being described. In no case does such identification imply recommendation or endorsement by the National Bureau of Standards, nor does it imply that the product identified is necessarily the best available for the purpose.

games, or sophisticated corporate spies, hoping to learn trade secrets or acquire the list of a competitor's top ten accounts. (See [PARKD 73A-B] and [PARKD 76A-B] for a discussion of computer crime.)

Current privacy legislation and increased public concern with the integrity and protection of data in such computer systems have made the problem of personal authentication most urgent. An example of such legislation is the Privacy Act of 1974 (5 U.S.C 552a). This act imposes numerous requirements upon Federal agencies to prevent the misuse of information about individuals and assure its integrity and security. (Guidelines for implementing this Act may be found in [FIPS 41].)

The technique of using passwords to authenticate a terminal user to a resource sharing computer system is well known. Nearly all systems in use in the Government, and all of the commercial timesharing systems, use this technique [ANDEJ 71]. However, passwords alone are not sufficient to guarantee system security. Rather, the use of passwords is one of many technical and procedural controls that can be used in concert with others as determined for a given system and its environment.

This report considers the generation of passwords and their effective application to the problem of controlling access to computer resources. After describing the need for and uses of passwords, the features of password schemes are categorized according to

- o selection technique
- o lifetime
- o physical characteristics
- o information content.

Password protection, both in storage and transmission, is dealt with in the next section, followed by brief sections on current implementations and cost considerations.

Security-related terminology used in this report is defined in [FIPS 39] and much of the networking and communications terminology may be found in [NEUMA 74]. For the convenience of the reader, selected terms from both works are contained in the glossary. Finally, an annotated bibliography of all referenced material is included.

It is not the intent of this report to provide formal guidelines for the effective utilization of passwords, but rather to bring together descriptions of the various techniques and their capabilities and limitations. Such a survey is a necessary first step for the generation of

appropriate guidelines for the effective use of passwords in controlling access to computer resources.

AUTHENTICATION

Typically when a user wishes to access resources on a remote computer system, he or she states a claimed identity, perhaps through typing a user name or identification number. The user is then required to verify the claimed identity. This latter process is referred to as personal authentication.

There are three basic methods by which a person's identity may be authenticated for the purpose of controlling access to a remote computer system:

- o something the person knows
- o something the person has
- o something the person is.

The first category includes, for example, passwords and lock combinations. Badges, ID cards, and keys fall into the second category; while "something a person is" includes characteristics such as one's appearance, voice, fingerprints, signature, and hand geometry. The advantages and limitations of these types of authentication techniques have been discussed extensively elsewhere [COTTI 75], [BROWP 76], [FIPS 48], [MUERJ 74].

During a 1972 workshop on controlled accessibility, an identification problem matrix (shown in Table I) was developed. This matrix identifies the elements of a computer system that might require mutual identification and authentication. The checks indicate the pairs chosen for discussion by the workshop [REEDS 74]. It is readily apparent that password techniques would be appropriate in several of these situations.

The actual authentication techniques selected for a given system should be determined by a cost-risk analysis. This requires consideration of potential threats, the probability of these threats occurring, and the expected losses resulting from a successful penetration of the system, versus the cost of providing data protection.

Password systems cost less at present than most of the other techniques for personal authentication. Consequently, it appears that passwords, perhaps in combination with other techniques such as badges or keys, will continue to be heavily utilized for some time.

Element being Identified \ Identifier	People	Terminal	Program	Data	Computer	O.S. Superviser
People		✓	✓			✓
Terminal					✓	✓
Computer		✓	✓		✓	✓
Program	✓		✓			✓
Data			✓			✓
O.S. Superviser	✓		✓			✓

TABLE I:

IDENTIFICATION PROBLEM MATRIX

USES OF PASSWORDS

Personal authentication may be required at any number of points along the path to accessing data. Such points include

- o entry to building
- o entry to terminal room
- o enabling terminal
- o encryption interface unit
- o login
- o file access
- o data item access.

Physical devices (e.g., cards, keys) are commonly used at the first three access points; while passwords, alone or in conjunction with other techniques, are commonly used at login, file access, or data item access time.

In addition to authenticating users to systems, password schemes may provide some protection against other types of threats. In their report on information privacy, Petersen and Turn [PETEH 67] describe types of threats against which passwords may be effective. These include the following:

1. browsing - using legitimate access to a part of the system to access unauthorized files,

2. masquerading - claiming the identity of an authorized user after obtaining passwords or other authentication items through wiretapping or other means,

3. between-lines entry - penetration of the system when a legitimate user is on a communications channel but not using his terminal,

4. piggy-back infiltration - interception of user-processor communications and the returning of messages that appear to the user to be from the computer system.

The degree to which passwords are effective against such threats varies greatly. They provide good protection against browsing when implemented at the file or data level. However, passwords are ineffective against the threats of between-lines entry and piggy-back infiltration unless used for every message (in the former case), or when used as a means of reverse (e.g., processor-to-user) authentication (in the latter case).

Carroll and McLellan [CARRJ 71] also discuss these threats as well as some countermeasures. Lientz and Weiss [LIENB 74] consider costs of implementing these countermeasures and levels of sophistication of the threats.

Data encryption keys and the banking community's Personal Identification Number (PIN) are forms of passwords when used as a means of verifying identity. An encryption key controls the algorithmic transformation (encryption) performed on data to render the data unintelligible. The PIN is typically a four-to-six-digit number assigned by the bank or selected by the cardholder. It is used in conjunction with a magnetically encoded card. Throughout this report analogies will be drawn among encryption keys, PIN's, and passwords.

In order to be an effective deterrent to corputer system penetration, a password should be

- o difficult to guess
- o easy for the owner to remember
- o frequently changed
- o well-protected.

The degree to which a password scheme incorporates these features determines the work factor necessary to compromise the password.

The following sections discuss password-related techniques and mechanisms which can be combined to create the appropriate password scheme for a given system.

PASSWORD SCHEMES

Password schemes differ according to

- o selection technique
- o lifetime
- o physical characteristics
- o information content.

In this section the types of password systems are discussed along with the threats against which they are most effective. Examples are presented. (See [WOODH 77] for another discussion of password techniques.)

Password Selection

A password may be chosen by the system user or assigned. User-selected passwords are far from secure since people tend to pick words or numbers that have some personal meaning (e.g., birthday, child's name, street address) and consequently are easy to guess [BEARC 72]. The primary advantage of a user-chosen password is ease of recall, alleviating the need for writing the word down.

Passwords may be assigned to users by the system security officer or by the computer system itself. Although assigned passwords are generally more secure than user-selected codes, their benefits may be nullified if they are written down by the user, taken from a master list which is discovered [WINKS 74], or generated by an algorithm that is deduceable [JOHNS 74].

Johnson examined the use of pseudorandom numbers as passwords and discovered that various "logistically attractive" periodic password generation systems are in fact vulnerable to simple number-theoretic analysis. The generating systems he considered were of the type

$$x_{n+1} = ax_n + b \pmod{2^u}, \quad u \tilde{=} 40,$$

where a and b are selected constants and x(sub n) is the nth password generated. This type of generating system would be considered attractive, for example, in a large system in which it is not practical to use complex password schemes. To reduce vulnerabilities of such schemes, Johnson proposes new password generation and distribution strategies that would help to ensure a higher degree of security, without significantly increasing the system costs. [JOHNS 74]

An example of a computer-generated password scheme is the random word generator developed to run on Honeywell's Multiplexed Information and Computer System (Multics) [GASSM 75]. The random word generator forms pronounceable syllables and concatenates them to create words. A table of pronunciation rules is used to determine the validity of each construct. This system was developed to enhance the security of some Multics installations, such as the Air Force Data Services Center (AFDSC).

The motivation for a pronounceable password generator is to make the assigned words easier to remember, thus lessening the temptation to write the words down. Of course, what is deemed pronounceable by one person, may be considered gibberish by another, even though the rules of grammar for the particular language are adhered to.

In order to enhance pronounceability, generated words may be presented to the user in hyphenated form. Examples of the words generated are

qua-vu
ri-ja-cas
te-nort
oi-boay
fleck-y.

Besides being easy to remember, the generated words must be difficult to guess. This requirement is satisfied by giving the program the ability to generate a very large set of possible words in a random fashion.

The random word generator is capable of generating words of any length. However, words of five to eight characters are recommended. Longer words tend to be less pronounceable, while shorter words result in too few available passwords for a given system and its user population.

At the Air Force Data Services Center the use of the password generator is not mandatory. To help lessen the problem of being given a password that to them is unpronounceable, users can reject the assigned password and try again. Under the current implementation they can also elect to provide their own passwords. After nearly eighteen months of operation of the password generator, it was observed that about 50% of the system users allow the system to assign their passwords.

In recognition of the need for password schemes that are secure against penetration attempts based on guessing, Bushkin states the following principle of computer security:

> No passwords or other user authentication data shall have been or shall be created or generated either by the human user who will use them or by a non-human agent (e.g., a program) of his creation or under his control...

The intent of such a rule is to thwart attempts at guessing the password. Furthermore, Bushkin indicates that nonhuman (automated) generation of passwords is the preferred method for enhanced system security. [BUSHA 75]

To assist users in remembering numeric passwords, portions of the password (e.g., groups of two digits each) could be associated with easily visualized objects. For example, the user could be assigned the number 2356, where the 23rd item on a list is a basketball and the 56th is a tire. Then the user could form a mental image of the two objects and use that image to more easily recall the true password. A list of ordered objects could be posted at each terminal, and by recalling the image the user could, if necessary, easily determine the password. Thus if, in the above example, 100 items were contained on the list, the total number of passwords possible would be 10,000. Of course in such a scheme the list would have to contain enough items to discourage trial-and-error attempts at determining passwords.

A consideration in password generation systems is the number of duplicate passwords assigned. Obviously, if the user space is large and very few users have the same password, then assuming that one password for one user is known, the likelihood of determining which other users have that password is small. For example, if five users out of 1,000 had identical passwords, the probability of a penetrator determining the other four users of the known password would be 4/999. Duplicate passwords need not be a problem, then, unless the number of duplicate passwords at any one time is large. However, the probability of a successful penetration of a system with even a small number of duplicate passwords assigned increases when the encrypted (i.e., algorithmically transformed) password table is available to the users. This latter case will be discussed in the section on password protection.

Password Lifetime

Current password schemes allow password assignments to be used for an indefinite period of time, for fixed intervals of time (e.g., one month), or for a single use only (one-time passwords). The length of time that a password remains in effect is called the password lifetime or period.

Passwords that remain in effect indefinitely (often called "fixed" passwords) are the most susceptible to compromise. Due to the length of time available, these passwords are especially vulnerable to exhaustive testing. Making the length of the password appropriately long, locking-out log-on attempts after several (e.g., three) tries [HELDG 76], and enforcing time delays between log-on attempts provide some defense against exhaustive password enumeration attempts [WEISC 69].

Another shortcoming of passwords with indefinite lifetimes is the difficulty in detecting a successful compromise of the password. Some systems prohibit a user from being logged onto the system from more than one terminal at a time [BEARC 72]. Others, such as the Monitor operating system for the DECSYSTEM-10, inform the user at log-on and log-off of the presence of other users with the same user name or identification number, and hence the same password. However, even if such system constraints are present, the odds of a system penetrator and the legitimate user attempting to use the same account at the same time depend upon the frequency and duration of access of each. Of course, to lessen the probability of detection in this manner, the penetrator may elect to use the system late at night when the legitimate user is presumably asleep.

As a deterrent against such threats, some systems (e.g., Multics at the Massachusetts Institute of Technology and TENEX at Bolt, Beranek and Newman, Inc.) include the last time logged on as a part of the banner (i.e., the informative messages displayed by the system whenever a user logs on). This presumably informs someone if such successful penetration has taken place.

An example of a system penetration that was successful over a period of 3 1/2 months was recounted in an August 1976 article in the Washington Post. This article detailed the successful penetration of a small computer firm's system by a former employee. In this case, the employee continued to use his old account and password after he ceased to be employed by the firm [POST 76].

Obviously more frequent password changes are desirable [WINKS 74], [ANDEJ 72]. An example of a system which requires password updates at fixed intervals of time is the Air Force Data Services Center. In this system, users are required to change their passwords every six months. The enforcing mechanism is the operating system.

One-time passwords are recognized as generally providing a higher level of protection [ANDEJ 72], [PETEB 67], [WEISC 69], [BROWP 74]. Successive passwords may be selected by the system from an internal list [WEISC 69],

generated by a program [GASSM 75], [JOHNS 74]. [BARAP 64], or selected from lists or cards previously distributed to authorized users [BEARC 72], [PETEB 67].

Anderson [ANDEJ 72], [ANDEJ 71] advocates the use of one-time password schemes. He contends that if passwords are changed each time they are used there is "no more risk in writing down the password than in carrying a key to a locked room." Should loss or theft occur, prompt reporting would minimize the risks involved. Of course, the legitimate user would have to access the system frequently in order to ensure the timely discovery of a successful system penetration.

As a means of further reducing the risk of carrying a password openly, Anderson suggests that the system could print a list of passwords for each user. Only one of the words on the list would be the actual password, and the exact location of the valid password could vary from user to user. He also mentions the possibility of encoding the new password on a magnetic card [ANDEJ 72].

The feasibility of using one-time passwords in conjunction with magnetically encoded cards was investigated by Richardson and Potter [RICHM 73]. In their design of a prototype system, the cardholder was required to key-in a secret password in addition to that read from the card. As has been noted previously, combinations of authentication techniques may provide a higher degree of security than systems incorporating only one such technique. Here, the use of a manually-entered password is necessary to prohibit unauthorized use of a lost or stolen card before the loss has been reported. Likewise, the password is of no use to a would-be penetrator without the card. It was noted in [ANDEJ 72] and [RICHM 73] that the major disadvantage of such a technique is the cost of the magnetic card reader/writer.

Lawrence Livermore Laboratory's OCTOPUS network uses a password scheme, similar to one-time passwords, incorporating a changing counter. A computer generates and authenticates all combinations (passwords). At each terminal session a counter associated with the combination is incremented and this new value is communicated to the user. Thus, the skipping of a value would imply that the combination had been used by someone else. [FLETJ 75]

One-time passwords are utilized in SWIFT (Society for Worldwide Interbank Financial Telecommunications), the world-wide banking system developed by the Burroughs Corporation. When a terminal is connected, the operator uses a four-digit, one-time password taken from a list which is supplied in two lists sent separately. For example, with

the following lists

LIST 1	LIST 2
1 2	4 5
3 7	9 8
4 6	3 5
.	.
.	.

the first password would be 1245. Additional security features in SWIFT include message sequence numbers and the generation of a four hexadecimal digit authenticator result. This latter number is generated by running the entire message text through the SWIFT authenticator algorithm. In addition, at log-out time the operator specifies the next log-in time. SWIFT will refuse any earlier log-in attempts.

Major drawbacks to the use of one-time passwords are the cost and difficulty associated with the distribution of lists to large numbers of users [ANDEJ 71] and with the support of users who get "out of step" in a system with a heavy workload [BEARC 72]. Beardsley illustrates this latter point by describing a heavily used administrative system with nearly 6000 users, 1300 terminals, and a half-a-million transactions on a given day. Of course in the previous two examples, which incorporated counters or incremented passwords, the distribution problem is minimized.

Petersen and Turn have noted that one-time password schemes alone are not effective against the threat of between-lines or piggyback entry. For protection against these threats, message authentication via attachment of one-time passwords to each message would be required. Encryption at the terminal level is also an effective protection mechanism in this situation. [PETEH 67]

Physical Characteristics

A password's physical characteristics include its size and makeup (i.e., the "alphabet" or set of characters from which it is made). The number of different passwords possible in a given scheme is called the password space.

The Personal Identification Number (PIN) used in conjunction with banking transaction cards is typically a four-to-six digit number; while some computer systems accept passwords eight or more characters in length, with both numbers, letters, and special characters (e.g., backspace, '@', vertical tab) being permitted.

Given a password of length L that is formed using any of the 26 letters in the English alphabet, there are 26**L (where the symbol '**' indicates the exponential) possible words of length L that could be generated. For example, the number N of all possible words of length 8 that can be formed from the English alphabet is 26**8, or approximately 2.1 X 10**11. The password space may, however, be somewhat larger if passwords of lengths up to L are permitted. Then the password space S becomes

$$S = \sum_{i=1}^{L} N^{i},$$

where N equals the number of characters in the alphabet. [HELDG 76] When conditions such as pronounceability are added to the scheme, then a fraction f of the total number of possible words would comprise the password space. Once we know f, then for a given length L we can calculate the number of pronounceable words n by

$$n = fN.$$

In the previously described pronounceable password system [GASSM 75], an estimate for f of .02653 was found for words of 8 letters. The resulting value for n was thus

$$n = .02653N = 5.540 \times 10^{9}.$$

Meissner [FIPS 48] emphasizes that, in order to adequately assess the security of a given password scheme, one must consider the number of allowable combinations for valid passwords, rather than simply the theoretical number of combinations based upon the size of the alphabet and the generated password.

In [ANDEJ 72] Anderson considers passwords generated as random strings of letters or numbers. He presents a formula for determining the random password length required to provide a given degree of protection against systematic testing. The assumption is that tests occur at the maximum line transmission rate, as would be the case if another computer were attempting penetration by exhaustive enumeration. In his formula, the password size is found by solving

$$(R/E)4.39 \times 10^{4} \; (M/P)^{S} \leq A \qquad (1)$$

for S, where S is the password size in characters. Here, R is the transmission rate of the line in characters per

minute, E is the number of characters exchanged in a log-on attempt, P is the probability that a proper password will be found, M is the period over which the systematic testing is to take place (in months of 24 hours per day operation), and A is the size of the alphabet from which the password is made.

As an example, Anderson determines the password size drawn from the English alphabet that gives a probability of no more than .001 of recovery after 3 months of systematic testing. He assumes a line speed of 300 characters/minute, and an exchange of 100 characters during a log-on attempt. The computation is as follows:

$$\frac{300}{100} \times 4.39 \times 10^{4} \times 3 \times 10^{3} \leq 26^{S} \qquad (2)$$

$$3.951 \times 10^{8} \leq 26^{S} \qquad (3)$$

$$26^{S} = 3.089 \times 10^{8} \text{ for } S=6 \qquad (4)$$

$$26^{S} = 8.03 \times 10^{9} \text{ for } S=7 \qquad (5)$$

Therefore, in this example S=7 is the reasonable choice. Note that increasing the alphabet to 128 characters (e.g., for 7-bit ASCII) reduces S to 5.

Although encryption keys can be considered authenticating mechanisms analogous to passwords, a determination of adequate key size is obviously based upon additional considerations. For example, Shannon notes that the size of the key space should be as large as possible, not only to discourage trial-and-error approaches, but to permit the assignment of unique keys to large numbers of users and to allow frequent key changes. [SHANC 49]

It should also be noted that the effectiveness of encryption as a protection mechanism does not depend solely upon the encryption key chosen, but rather upon

1. the algorithm employed,

2. the implementation of the algorithm (e.g., when does encryption take place),

3. the criteria used in selecting the key (e.g., if an algorithm supports a key space of 2**56, but encryption keys of only four digits are used, then the effective key space is drastically reduced).

Information Content

The password may provide information in addition to personal authentication. The University of Western Ontario's generalized information retrieval system (GIRS) incorporates the use of assigned, functional passwords whose contents reveal the users' authorization levels [CARRJ 71A]. In particular, these passwords determine:

1. which subset of available processing functions can be exercised;

2. which portions of records can be operated upon by these functions; and

3. which records the user is privileged to work with, or conversely, which records the user is prohibited from using.

Note that in this system an additional password is needed for authentication; the functional password is used by the information retrieval system to assess a user's authorization level or capabilities. This is not to indicate, however, that both functions could not be provided by one password, used only at logon time.

Besides imparting authorization information, it has been suggested that passwords could be constructed to contain check digits or some other sort of self-checking code. "Check digitry" is already being successfully used in other environments, as discussed in a series of articles by Alan Taylor [TAYLA 75 A-B], [TAYLA 76]. In one example reported by Taylor [TAYLA 75A]:

> The Pennsylvania Bureau of Sales and Use Tax some time ago adopted a Modulo-10 check digit to safeguard a seven-digit number. The technique it selected was to multiply the first digit by 7, the second by 6 and so forth until the last digit was multiplied by 1. It then used the Modulo-10 complement of the answer as the check digit and placed it after the seventh number.

the computation would appear as follows:

```
Account Number:      1 9 3 4 2 6 7
Multipliers:         7 6 5 4 3 2 1
Check Digit Computation:

   1 x 7 =  7
   9 x 6 = 54
   3 x 5 = 15
   4 x 4 = 16
   2 x 3 =  6
   6 x 2 = 12
   7 x 1 =  7

   Total = 117
   Mod-10 = 7
   10 Complement = 3
```

Thus, the resulting check digit for 1934267 is 3.

Techniques such as this, combined with some elementary analysis, could help more sophisticated password systems discriminate between entry-errors (such as transpositions of digits) and actual penetration attempts, especially attempts via exhaustive testing.

This idea is similar to that embodied in Kaufman and Auerbach's general model of an electronic funds transfer system. This system incorporates the use of cryptographic check digits derived from the PIN [KAUFD 76].

Handshaking Schemes

Other types of authentication schemes which may provide a higher degree of security than lower level schemes such as fixed passwords are those incorporating the execution of an algorithm for authentication. Such procedures are often referred to as "handshaking" or "extended handshakes" [CAMPH 73], [BEARC 72]. Some of these procedures directly involve the use of passwords; others can only marginally be considered password schemes.

The ADEPT-50 time-sharing system incorporates a handshaking scheme [WEISC 69]. In order to gain admittance to the system, the user must supply information items including user identification, password, and accounting data. The terminal identification is also compared against the terminal id list for which the user id was franchised.

Although not a password scheme, Hoffman's formulary model is also considered an example of an extended handshake access procedure [HOFFL 71]. Formularies are sets of access control procedures which grant or deny access to data at data-access time, rather than at file-creation time. This is as opposed to control provided by most password schemes

in which passwords are associated with files.

In several systems, handshaking is accomplished by a dialog between the system and the user. In such procedures the user may be required to answer questions (e.g., cat's name, astrological sign) asked in a semi-random fashion, or to supply additional passwords and/or account information [LUPTW 73]. This is analogous to having several passwords, any number of which may be requested in any order. It is even conceivable that the questions themselves could be chosen by the system user.

In another variation, credited to Les Earnest by [HOFFL 69], the handshaking is accomplished by both the system and user performing a transformation on a given number and comparing the results. The system presents the user with a pseudorandom number and requires that the user perform a specified mental transformation T on that number. The result is then sent back to the computer, which performs an appropriate transformation and compares the results. Thus, the user has performed T on a number x and transmitted y=T(x). Consequently, an eavesdropper monitoring the transmission would at most see x and y. Note that the latter transformation need not be the inverse of the former transformation, but may be any suitable (e.g., non-degenerate) calculation whose results are dependent upon the user-transformed value.

Hoffman asserts that even "simple" T's such as

$$T(x) = [(\sum_{i \text{ odd}} \text{digit } i \text{ of } x)^{3/2}] + (\text{hour of the day})$$

raise the work factor in breaking the scheme significantly. Of course in such a system the transformation itself would still have to be kept secret by each user.

PASSWORD PROTECTION

The previous section has been concerned with the selection of a password scheme that, in addition to being convenient to use, is secure from discovery through guessing or exhaustive enumeration. However, regardless of the password scheme implemented, protection of the password (or authenticating algorithm) is vital.

We can assume that authentication algorithms or handshaking procedures are guarded by the system's full array of protection mechanisms. (Note that if a penetrator succeeds in gaining access to the algorithm under these conditions, then he could just as easily access any other files in the system!)

The three times during which the password must be protected, are

- o initial distribution
- o storage
- o entry and transmission.

In this section we shall consider the requirements for guarding the passwords against potential threats that might occur at such times.

Initial Distribution

The initial distribution of passwords to users is one aspect of password assignment, selection, and transmission. Two items must be considered in this situation:

- o user identification
- o distribution method.

It is usually the practice that first-time users of a system make application in person for authorization to use the system resources. At that time a temporary password can be given to the user. The user then has the responsibility for logging onto the system and changing the password to one known only to him.

In another form of password distribution, more useful when users are great distances from the computing facility, the password is transmitted by mail to the user. PIN's are normally distributed in this manner. If more assurance of receipt is required, registered mail or special messengers can be used.

Initial distribution of encryption keys could be handled in a similar manner; with the magnetic card bearing the first key being sent via registered mail.

Password Storage

Most password schemes employ the use of tables or lists which contain the current password for each authorized system user. (A notable exception would be the user-transformation scheme described above [HOFFL 69].) As these tables and lists are perhaps the most vulnerable part of a password system, efforts should be taken to protect them.

In recognition of the vulnerability of tables and lists associated with authentication techniques, Bushkin [BUSHA 75] includes the following principle in his set of design requirements:

> All passwords and authentication data shall be stored in an irreversibly transformed state.

R. M. Needham is credited with being the first to recognize the vulnerability of password lists. An encipherment algorithm attributed to him has been implemented at Cambridge, England. As opposed to ordinary communications ciphers in which the enciphering and deciphering algorithms are of nearly equal complexity, the cipher produced by this algorithm is a "one-way cipher." This is a cipher for which no simple deciphering algorithm exists. In such a scheme, the user's password is encrypted as soon as it is received by the system, and the transformed password is then compared with the encoded table entry. [WILKM 75]

A discussion of Needham's system and the merits of various others can be found in [EVANA 74]. Purdy [PURDG 74] also describes the Needham scheme, discusses the selection of good one-way ciphers, and suggests the use of polynomials over a prime modulus.

Lawrence Livermore Laboratory's OCTOPUS network also incorporates password table encryption. Fletcher notes that if an encrypting algorithm is chosen so that attempts to break it by cryptanalysis would be as time-consuming as by trial-and-error methods, then there would be no real need to protect the encrypted password table. However, in the OCTOPUS network, the password table is protected. [FLETJ 75]

There are still potential threats involved in such schemes. One is the interception of passwords prior to encryption, and another is the selection of a poor cipher. The former problem will be dealt with in the next section.

An example of a poor cipher would be one that is highly degenerate (i.e., one in which many combinations encrypt to the same value) [FLETJ 75]. Under such a scheme the simple exposure of the encrypted list could give enough information to a would-be penetrator to allow him to, if not break the algorithm, at least access the files of any users whose passwords in their encrypted form were identical to his. Note that this is also the case when several users of a system have identical passwords.

As a part of their Multics vulnerability analysis, the Air Force considered the threat of exposure of password files [KARGP 74]. Their report suggests that accessing the system password file could be of minimal value to a system penetrator. Assuming that the password file is the most highly protected file in the system, anyone who succeeded in accessing this file could conceivably penetrate <u>any</u> other file in the system!

For completeness the Air Force study did analyze the "non-invertible" encipherment scheme used at that time by the Multics system. In a report soon to be published, the details of their successful penetration of that scheme will be detailed [DOWNP 77]. Basically, the approach was to assume that although Multics would accept passwords up to 8 characters in length, most individuals would use words less than 6 characters long. Proceeding with the assumption of trailing blanks, the scheme was broken for passwords of this size. After developing a solution for this special case, they then succeeded in developing a general solution. As a result of this study, the Air Force has provided a "better" password scrambler that is now used in Multics.

Not all operating systems read-protect encrypted password tables. Bell Laboratories' UNIX timesharing system, for example, currently allows users to read the password table in which user passwords are stored in encrypted form. The assumption here is that password encryption alone provides adequate protection.

This protection, however, is not entirely dependent upon the algorithm used. If both the password table and the encryption algorithm are available, then even if the passwords are difficult to decrypt (i.e., a "one-way" cipher is used) one could reasonably hope to derive them by exhaustive enumeration. For example, the encrypted password table could be copied to another computer system and compared against the outputs of the same algorithm when run against all words of five or less alphabetic characters. The use of larger, more frequently changed passwords could thwart such attempts.

Note that if key-oriented algorithms (such as the Federal Data Encryption Standard) are used, access to the password table and knowledge of the encryption algorithm alone are not sufficient to obtain the passwords. Either the key itself would have to be exposed, or an unencrypted password and its encrypted form would have to be obtained. In this latter case, the encryption key would still have to be derived, and a larger sample of encrypted and unencrypted text would probably be needed.

In some systems using magnetically encoded cards, the PIN itself is stored on the card in an encrypted form. There are currently two methods for protecting these PIN's:

1. The PIN and other account-related data are encrypted and encoded on the card. In off-line systems using this scheme, the terminal is then responsible for decrypting the data and comparing the customer-entered number with the PIN.

2. In other systems, the PIN is not encoded at all, but instead has a predetermined arithmetic relationship to such data as the account number which is encoded on the magnetic card.

In an article discussing the threats to bank card systems [NORTE 75], Industrial National Bank Vice President Ernest Northup describes the components of a card-based electronic funds transfer system (EFTS) and notes that the "use of a standard PIN scrambling technique or algorithm for bank interchange would require that its elements be widely know, at least among equipment vendors. This increases its vulnerability." He catagorizes a secure PIN system as one utilizing a technique that

1. demonstrates its resistance to cryptanalysis mathematically,

2. does not require direct exposure of the PIN during transmission, and

3. can be physically protected from analysis within the device in which it is contained.

Kaufman and Auerbach present a comprehensive set of EFTS security principles. Concerning the storage of PIN's they state that "there should be no way to derive the PIN from information on the card," although they observe that many current schemes are based upon techniques for deriving the PIN from information on the card. PIN storage on the card does reduce the need for storage in the system;

however, it is extremely risky. With such a scheme, the incentive for theft of the algorithm for deriving the PIN is high since, once the algorithm is obtained, all PIN's can be derived for the entire system! [KAUFD 76]

Password Transmission

Passwords are vulnerable to several threats during their transmission from terminal to computer. Potential threats include wiretapping, electronic eavesdropping, and piggyback infiltration. The password may also be discovered later in the trash if a hardcopy terminal was used, or observed on a CRT screen immediately after entry. These latter two problems are usually dealt with by masking (the over-printing or under-printing of a series of characters) or echo-suppression. However, as pointed out by Carroll and McLellan [CARRJ 71B], in general the "use of a mask affords no protection to users on CRT visual display terminals." Furthermore, echo suppression is meaningless when the keyboard input is printed directly, as in half duplex mode, rather than echoed. Another method sometimes used as a countermeasure against such forms of password detection is the use of non-printing characters as a part or all of the password [FIPS 48],[HELDG 76]. In some half-duplex systems there exist print/display suppress keys which can be used at the terminal to locally inhibit the display of the password.

In a discussion of piggyback infiltration, Carroll and Reeves described a situation in which unsuspecting terminal users could be "exploited by a process which mimics the real system long enough to obtain a password..." [CARRJ 73]. Of course, echo-suppression and masking are of no help in countering this type of threat. Furthermore, if a more intelligent device than a conventional (i.e., non-intelligent) terminal is used to intercept the conversation, then non-printing characters also lose their effectiveness.

The user-transformation schemes described by [HOFFL 69] and [CARRJ 70] are one way of effectively shielding the password in transit. Here the user, when presented with a random number, performs a pre-determined transformation on it and transmits the result back to the computer for verification. The incorporation of a date-time group into this transformation is recommended to provide additional protection against piggyback infiltration [CARRJ 70]. User-transformation schemes, however, would seem to be costly, particularly if there is to be some variability among the users.

Another method for password transmission can be found in Babcock's description of the RUSH timesharing system [BABCJ 67]. Here mention is made of a "dial-up and

call-back" system in which the user is directed to telephone the password to the computer system operator when access is requested to very sensitive files. Although this technique might afford a degree of protection for the password, it obviously would not be appropriate for a large, heavily used system.

A similar technique that can be used involves the computer breaking the communications link, and then placing a call to the terminal. This procedure ("call back") is useful for verifying that an authorized terminal is being used; however, this alone is not sufficent to verify user identity.

Optimal protection of the transmitted password, as with any data, can be realized by encryption of the communications link during the entire conversation [BARAP 64], [BRAND 75]. (The Federal Data Encryption Standard would be suitable for this purpose [FIPS 46].) Communications systems incorporating the use of encryption are currently in use in the non-military environment. In one such system, a banking institution uses hardware code scramblers to protect customer passwords in transit. In this application, the customer selects a 16 character password, which is then scrambled twice before reaching the computer where it is filed as a six-digit code. The scrambling, which is claimed to be irreversible, is handled by integrated circuits built into relay boxes at the terminals and computer center [NEWS 76].

Branstad notes that encryption keys and authentication codes may be in effect the same item. In his proposed network access control machine, these keys are never transmitted through the network, but rather are loaded simultaneously by interface units into a primary encryption device. Thus, authentication can be considered complete at that level (at least) if a message can be encrypted, transmitted, and correctly decrypted [BRAND 73],[BRAND 75].

In a master's thesis on encryption-based protection protocols, Stephen Kent considers encryption key distribution [KENTS 76]. He identifies two basic transmission techniques:

- o chained key changes
- o two-level key distribution systems.

Under the chained key system, each new key is enciphered using the last key issued. This new key is then used until another change occurs. Under the two-level distribution system, a special key is used solely for transmitting new keys to remote users. Kent describes protocols for using these two schemes and considers the use

of magnetically encoded cards for distribution of keys. He presents the following example of a login sequence incorporating two-way authentication:

1. The user enables the terminal and establishes a connection to the host.

2. The host responds in cleartext confirming the connection by sending the host name.

3. The user transmits in cleartext the login identifier, and then inserts a magnetic stripped plastic card containing his or her (primary) key and enables the encryption module.

4. The host locates the user's primary key using the login identifier presented in cleartext. A new (secondary) key to be used during this session is then created and transmitted using the standard key change protocol.

5. The terminal deciphers the key change messages and loads this secondary key. The host switches simultaneously to this new key. The terminal then transmits a message confirming key receipt and the host, upon receipt of the confirmation, is ready to engage in secure communication with the user. All communication from this point on will be carried out using the new key.

Additional steps involve transmission of the current time and date, enciphered using the new key, to the user. Such a login protocol not only succeeds in authenticating the user's identity to the system, but also confirms the system's identity to the user, thus proving an effective means of protection against such threats as piggyback infiltration and between-lines entry.

Again considering the EFT environment, Kaufman and Auerbach [KAUFD 76] present the security principle that the "exposure of PIN's should be minimized during a transaction." In their general design for a local EFT system, they include a provision for one-way PIN transformations. The PIN in clear form is neither transmitted nor stored anywhere in the system.

CURRENT IMPLEMENTATIONS

Computer hardware and software vendors are responding to the demand for enhanced system security [IBM 74A-G], [HAMMC 73], [JARVJ 74], [McCRR 73]. Their efforts in the software area can be categorized as those involving

- o operating system modifications
- o add-on packages.

Current implementations of password systems have been described in [BUSHA 75], [CARRJ 71A-B], [FLETJ 73], and others. Several of these are discussed in this report. In all of these systems, the password facility was built into the operating system or data base management system.

Recently, in response to the demand for more secure computer systems, vendors have made available add-on security packages. Examples of such systems are those marketed by IBM Corporation and Tesseract Corporation. Other manufacturers and software vendors may offer similar packages.

IBM markets a package called the Resource Access Control Facility (RACF) which is supported by their MVS operating system. The purpose of RACF is to assist computer installations in controlling user access to data sets on direct access storage devices. It performs three major functions:

1. user identification and verification - identifies and verified a RACF-defined user to the system during TSO logon and batch job initialization.

2. authorization checking - determines if a user is permitted to access a RACF-protected data set.

3. logging - writes records to SMF (System Management Facilities) and routes messages to the security console following the detection of (1) unauthorized attempts to enter the system, and (2) authorized or unauthorized accesses to RACF-protected data sets.

Descriptions of RACF, ranging from a product announcement to technical description, may be found in [IBM 76 A-C].

IBM also offers an installed user program called the TSO/Codes Update System [IBM 76D-E]. This package features

1. fully-automated password update,

2. date-oriented construction of passwords utilizing randomizing routines which should not create duplicate passwords in a 100-year period,

3. facility for initial distribution of passwords using mailer-type forms.

Tesseract Corporation has developed the Data Access Security System (DAS), versions I and II. DAS I operates on all versions of the IBM Operating Systems OS MFT/MVT, VS1 and VS2 (SVS/MVS), including HASP, ASP and TSO. It is described as an improvement upon IBM's password facility that "makes the facility more generally usable and prevents the unauthorized disclosure of passwords" [TESSE 76A]. In contrast to DAS I, which built passwords from components of the Job Control Language and then provided them to the existing password facility, DAS II is a rewrite of IBM's password facility [TESSE 76B]. Its features include the support of shared password data sets and the ability to restrict

1. the number of accesses to a protected data set,

2. accesses to a particular period of time,

3. access to batch jobs only, or TSO users only,

4. access to specific jobs, TSO users, programs and job accounting parameters.

These are only a few examples of the types of add-on security packages available. With the continually increasing emphasis being placed upon computer security and data integrity, it is likely that packages such as these will continue to appear, until more operating systems, designed with security in mind from the beginning, are developed.

COST CONSIDERATIONS

The costs of a given password scheme are those incurred by the intruder as well as by the protector. These costs must be considered in conjunction with the value of the information to be protected. (See [TURNR 72], for a discussion of the value of personal information in qualitative terms.)

The costs to the protector include not only the hardware and software costs involved, but also the effect on overall system performance. For example, the amount of processing time required and the degree of communications channel loading may result in severely degraded system response time.

Lientz and Weiss [LIENB 74] consider the implementation costs of various security measures in a computer networking environment. For costs related specifically to password schemes, they include the following:

1. Simple password for identification: cost of software, systems performance, storage.

2. Changeable passwords: cost of software, updating lists and storage, systems performance.

3. Password transformations: cost of software, cost of random lists and storage, systems performance, computational cost.

4. Magnetically encoded cards with constant or changeable passwords: cost of terminal to read/write, cost of software, systems performance.

Nielsen et al also consider password-related costs in a comprehensive report which focuses on the identification and analysis of computer system integrity safeguards [NIELN 76]. Among the password-related controls addressed are password protection, change, amplification, generation, penetration detection, compromise detection, and print suppress. The annual costs (e.g., implementation, operation, and overall) of each safeguard are indicated as being small, moderate, or large; and the effectiveness of each in the prevention, detection, and reduction of computer system integrity violations is judged.

Password schemes which involve authentication to the file or data item level are more costly than systems employing passwords only at log-on. In a report on the principles and costs of privacy protection in databanks, Turn observes that the "costs of access control operations

reflect themselves in increased processing time and storage space requirements". He relates the results of a study of these costs which revealed a 22 to 140 percent processing time increase in file access operations, depending upon when access controls are applied (e.g., at file open time, or data item access time) [TURNR 74].

Since add-on security packages are becoming available, cost of such "retrofit" techniques must be considered. The total cost of such systems includes not only the purchase or lease price, but also the cost of any additional hardware and programmer time needed to install and support the system.

The cost to the system intruder includes the investment in time and equipment (i.e., the work factor) necessary to, in this case, determine the password or password-generating algorithm. Risk can also be considered part of the penetration cost.

As an example, consider the intruder's costs of acquiring passwords through wiretapping. These could range from the cost of recording equipment (a few dollars), to the cost of a minicomputer and associated software development (several thousand dollars). Risks include possible legal prosecution [TURNR 72].

As aptly stated by Petersen and Turn [PETEH 67], "the level of work factor which is critical for a given information system depends, of course, on an estimate of the magnitude of threats and of the value of the information." They suggest that a work factor of one day of continuous computation required to break a single encryption key might be adequate against low-level threats.

Of course, the cost of the system utilized in the penetration effort must also be considered in order to better estimate the work factor required. That is, one day of continuous effort by a person with a hand calculator is hardly comparable with a day's effort by a large-scale computer system. For example, at a recent NBS workshop [MEISP 76] the following problem was chosen: the design of a large-scale digital machine which could be used for recovering the key used for encrypting data under the [at that time] proposed Federal Data Encryption Standard (DES). The results of that study indicated that to achieve key exhaustion time on the order of one day, the estimated cost would be several tens of millions of dollars, and that such a machine could not be placed in operation before 1990.

Thus it would appear that with the encryption key for the DES taking the place of the traditional password as a means of personal authentication, nearly optimal protection against exhaustive enumeration attempts can be achieved.

CONCLUSIONS

Although automated personal authentication techniques such as fingerprint, voice, and signature recognition are becoming less expensive and more accurate, it is apparent that the majority of commercial and Government time-sharing systems are continuing to rely upon passwords. We have shown that passwords can be an effective form of personal authentication when care is taken in their selection and protection. The features of password schemes have been categorized, their capabilities and limitations identified, and points at which password protection mechanisms are needed have been indicated.

Table II briefly summarizes some of the advantages and disadvantages of the various types of password schemes which have been examined here. Based upon these and other considerations presented in this report, it is apparent that a configuration providing a high level of security would be one incorporating passwords that are

- o one-time
- o computer generated
- o fairly unique
- o at least four characters long
- o random
- o encrypted when stored
- o encrypted in transmission.

Additional safeguards include the use of techniques such as banner lines to inform users of previous attempts (both successful and unsuccessful) at logging onto their accounts.

The exact password scheme appropriate for a given system depends, of course, upon the required level of security as determined by cost-risk analysis. Formal guidelines for the selection of appropriate password schemes and for the use of passwords in conjunction with other authentication techniques are needed.

It should also be noted that any emphasis on personal authentication in support of access controls should not result in the neglect of other technical and procedural controls such as logging, journaling, and authorization checking [BROAI 74]. For example, the certainty that there is a record of activities of a user's terminal session may often prove to be more of a deterrent to computer abuse than would system-imposed restrictions on what a user is authorized to do.

Until other forms of personal authentication become more cost-effective, the password will remain the most widely used means of controlling access to remote computing systems and services. With careful selection of appropriate password schemes and attention to password protection, both in transit and storage, it can be an effective personal authentication mechanism.

PASSWORD SCHEME	SOME ADVANTAGES	SOME DISADVANTAGES
SELECTION PROCESS:		
USER-SELECTED	EASY TO REMEMBER	OFTEN EASY TO GUESS
SYSTEM GENERATED	DIFFICULT TO GUESS	MORE DIFFICULT TO REMEMBER; GENERATING ALGORITHM MAY BE DEDUCIBLE
LIFETIME:		
INDEFINITE	EASY TO REMEMBER	MOST VULNERABLE TO EXHAUSTIVE ENUMERATION AND GUESSING ATTEMPTS; DIFFICULT TO TELL IF PASSWORD STOLEN
FIXED	EASY TO REMEMBER IF TIME INTERVAL IS FAIRLY LONG (E.G., WEEK OR MONTH); MORE SECURE THAN INDEFINITE (SHORTER TIME INTERVAL, BETTER THE SECURITY PROVIDED)	VULNERABILITY DEPENDS UPON TIME INTERVAL
ONE-TIME	USEFUL FOR DETECTING SUCCESSFUL PENETRATION OF SYSTEM; SHORT LIFE-TIME PROHIBITS EXHAUSTIVE TESTING	DIFFICULT TO REMEMBER UNLESS WRITTEN DOWN; VALID USER LOCKED OUT IF SUCCESSFUL PENETRATION OCCURS
SIZE AND ALPHABET:	LARGER THE PASSWORD AND ALPHABET, THE MORE DIFFICULT TO GUESS; LESS NEED FOR DUPLICATION OF PASSWORDS	LARGER THE WORD, MORE DIFFICULT TO REMEMBER AND MORE STORAGE REQUIRED
INFORMATION CONTENTS: (E.G., AUTHORIZATION INFORMATION AND CHECK DIGITS)	COULD AID DETECTION OF PENETRATION ATTEMPTS IF PENETRATOR UNAWARE OF VALID PASSWORD STRUCTURE	MAY CAUSE PASSWORDS TO BE LONG AND THUS MORE LIKELY TO BE WRITTEN DOWN; IF SCHEME BECOMES KNOWN, PASSWORDS COULD BE EASY TO DEDUCE
HANDSHAKING SCHEMES: (E.G., DIALOGS, USER TRANSFORMATIONS)	RESISTANT TO EXHAUSTIVE ENUMERATION ATTEMPTS; PROVIDES SOME PROTECTION DURING TRANSMISSION	MAY BE TIME CONSUMING; REQUIRES MORE STORAGE SPACE THAN SINGLE PASSWORDS

TABLE II: PASSWORD CHARACTERISTICS

GLOSSARY *

access

The ability and the means necessary to approach, to store or retrieve data, to communicate with, or to make use of any resource of an ADP system.

access control

The process of limiting access to the resources of an ADP system only to authorized users, programs, processes, or other ADP systems (in computer networks). Synonymous with controlled access, controlled accessibility.

access control mechanisms

Hardware or software features, operating procedures, management procedures, and various combinations of these designed to detect and prevent unauthorized access and to permit authorized access to an ADP system.

active wiretapping

The attaching of an unauthorized device, such as a computer terminal, to a communications circuit for the purpose of obtaining access to data through the generation of false messages or control signals, or by altering the communications of legitimate users.

add-on security

The retrofitting of protection mechanisms, implemented by hardware or software, after the ADP system has become operational.

authentication

(1) the act of identifying or verifying the eligibility of a station, originator, or individual to access specific categories of information.

(2) A measure designed to provide protection against fraudulent transmissions by establishing the validity of a transmission, message, station, or originator.

---

* Except as noted, all terms in this glossary have been selected from [FIPS 39] and [NEUMA 74].

authorization

The granting to a user, a program, or a process the right of access.

between-the-lines entry

Access, obtained through the use of active wiretapping by an unauthorized user, to a momentarily inactive terminal of a legitimate user assigned to a communications channel.

browsing

Searching through storage to locate or acquire information, without necessarily knowing of the existence or the format of the information being sought.

call back

A procedure established for positively identifying a terminal dialing into a computer system by disconnecting the calling terminal and reestablishing the connection by the computer system's dialing the telephone number of the calling terminal.

(computer) network

An interconnection of assemblies of computer systems, terminals and communications facilities.

cost-risk analysis

The assessment of the costs of potential risk of loss or compromise of data in an ADP system without data protection versus the cost of providing data protection.

cryptanalysis

The steps and operations performed in converting encrypted messages into plain text without initial knowledge of the key employed in the encryption algorithm.

cryptography

The art or science which treats of the principles, means, and methods for rendering plain text unintelligible and for converting encrypted messages into intelligible form.

decrypt

To convert, by use of the appropriate key, encrypted (encoded or enciphered) text into the equivalent plain text.

encryption algorithm

A set of mathematically expressed rules for rendering information unintelligible by effecting a series of transformations through the use of variable elements controlled by the application of a key to the normal representation of the information. Synonymous with privacy transformation.

formulary

A technique for permitting the decision to grant or deny access to be determined dynamically at access time, rather than at the time of creation of the access list.

handshaking procedures

A dialog between a user and a computer, a computer and another computer, a program and another program for the purpose of identifying a user and authenticating his identity, through a sequence of questions and answers based on information either previously stored in the computer or supplied to the computer by the initiator of dialog. Synonymous with password dialog.

host computer

A computer attached to a network providing primarily services such as computaton, data base access or special programs or programming languages.

identification

The process that enables, generally by the use of unique machine-readable names, recognition of users or resources as identical to those previously described to an ADP system.

impersonation

An attempt to gain access to a system by posing as an authorized user. Synonymous with masquerading, mimicking.

journaling

A complete recording of a set of facts which can later be used to reconstruct the data base [BROAI 74].

key

In cryptography, a sequence of symbols that controls the operations of encryption and decryption.

link

(1) Any specified relationship between two nodes in a network. (2) A communications path between two nodes. (3) A data link.

logging

A recording of a small set of facts concerning an access of data. A log should provide enough data so that an audit can uncover possible misuse and discover the responsible party. [BROAI 74]

masquerading

Synonym for impersonation.

password

A protected word or a string of characters that identifies or authenticates a user, a specific resource, or an access type. Synonymous with keyword.

piggy back entry

Unauthorized access that is gained to an ADP system via another user's legitimate connection.

risk analysis

An analysis of system assets and vulnerabilities to establish an expected loss from certain events based on estimated probabilities of the occurrence of those events.

terminal

(1) A point in a communications network at which data can either enter or leave. (2) A device that permits data entry into or data exit from a computer system or computer network, e.g., a data capture device, a teletypewriter, a remote job entry device, or a computer. Terminals may accommodate data in human or

machine readable form.

work factor

An estimate of the effort or time that can be expected to be expended to overcome a protective measure by a would-be penetrator with specified expertise and resources.

SELECTED BIBLIOGRAPHY

[ANDEJ 71] Anderson, James P., "On Centralized Distribution of One-time Passwords in Resource Sharing Systems," James P. Anderson and Co., Fort Washington, Pa., August 1971, 8p.

This note describes a centrally distributed, one-time password scheme for personal authentication of users in a computer resource sharing environment. The author postulates that under the conditions described, the protection of the password itself is unnecessary. A risk analysis of open one-time vs. 'secret' passwords is included.

[ANDEJ 72] Anderson, James P., "Information Security in a Multi-user Computer Environment," Advances in Computers, Vol. 12, 1972, Academic Press, Inc., New York, p. 1-36.

This article presents the problems and issues of protecting information in multi-user systems. Included are discussions concerning techniques of system access control, operating systems security, file protection, communications, and security assurance.

[BABCJ 67] Babcock, J.D., "A Brief Description of Privacy Measures in the RUSH Time-sharing System," Proceedings of the Spring Joint Computer Conference, Vol 30, 1967, p. 301-302.

As the title states, this article is quite brief. However, it does identify the main security-related features contained in the operating system. Included are such capabilities as a LOGIN statement providing three levels of protection to help prohibit unauthorized access; enhanced file protection; security enhancements in an RJE environment; and use of memory-protection features.

[BARAP 64] Baran, Paul, On Distributed Communications: IX. Security, Secrecy, and Tamper-free Considerations. Rand Corporation, August 1964, AD-444 839, 39p.

This is an early, comprehensive treatment of security in data communications networks. Emphasis is on cryptography, with sections devoted to key management.

[BEARC 72] Beardsley, Charles W., "Is Your Computer Insecure?" IEEE Spectrum, (January 1972), p. 67-78, 16 refs.

This is a survey of hardware and software techniques for helping to ensure computer security and data integrity. Topics covered include remote-terminal access, cryptography, communications, threat monitoring, processing controls, certification, and the internal audit.

[BRAND 73] Branstad, Dennis K., "Security Aspects of Computer Networks," Proceedings of AIAA Computer Network Systems Conference, American Institute of Aeronautics and Astronautics, New York, N.Y., April 1973, 8p.

The problem of defining the communication and switching requirements of a network of different computers, terminals, and users with various access authorizations is described. The impact that security requirements have on a network and some possible approaches to a solution are also discussed. Identification and authentication are contrasted and the use of passwords in conjunction with other authentication techniques is mentioned.

[BRAND 75] Branstad, Dennis K., "Encryption Protection in Computer Data Communications," Proceedings of the Fourth Data Communications Symposium, IEEE Computer Society, October 1975, p. 8-1 - 8-7, 2 refs.

An encryption algorithm for use in computer data communications is presented, along with the security requirements that are satisfied by proper use of the algorithm. Also discussed is the use of a network access control machine (NAC) to enforce access restrictions for the network. Among the functions of the NAC are the following: user identification and authentication, terminal/computer identification and authentication, and issuance of data encryption keys.

[BROAI 74] Broadman, I.S., "Protection Techniques in Data Processing Systems to Meet User Data Security Needs," (IBM Corporation, Gaithersburg, MD), Proceedings of the Second International Conference on Computer Communication, (Stockholm, Sweden, August 12-14, 1974), 1974, p. 485-489, 2 refs.

This paper defines and discusses four categories of computer data security protection techniques: physical protection, personnel practices, administrative procedures, and computer technology. Operating system integrity, user identity verification, authorization definition and checking, logging and journaling, and cryptography are described and discussed.

[BROWP 74] Browne, Peter S., "Security in Computer Networks," Approaches to Privacy and Security in Computer Systems, (Proceedings of conference held at National Bureau of Standards, March 1974), September 1974, NBS Spec. Pub. 404, p. 32-37.

Safeguards and solutions to problems of security and privacy are proposed and a model set of specifications for requesting secure computer services or systems is presented. The generation, protection, and uses of passwords are addressed.

[BROWP 76] Browne, Peter S., "Computer Security - A Survey," Proceedings of the National Computer Conference, AFIPS Press, Montvale, N.J., 1976, p. 53-63, 134 refs.

This brief paper highlights the major subtopics of interest to those concerned with computer security. A carefully selected, annotated bibliography is included.

[BUSHA 75] Bushkin, Arthur A., A Framework for Computer Security, System Development Corporation, McLean, Va., AD-A025 356, June 1975, 158p.

This report presents an overview of the computer security problem and an interrelated set of axioms and principles of computer security as the beginning of a top-down, structured approach to the computer security problem.

[CAMPH 73] Campaigne, Howard, and Hoffman, Lance J., "Computer Privacy and Security," Computers and Automation, 22:7, (July 1973), p. 12-17, 6 refs.

Physical, administrative, and technical safeguards for facilitating computer system security and control are discussed. Types of password schemes are given, with a brief discussion of some of the advantages and disadvantages of each.

[CARRJ 70] Carroll, J. M., and McLelland, P.M., "Fast 'Infinite-key' Privacy Transformation for Resource-sharing Systems," Proceedings of the Fall Joint Computer Conference, AFIPS Press, 1970, p. 223-230, 12 refs.

This paper describes a real-time software system for privacy transformation (encryption), presented within the context of known threats to privacy, available counter-measures, and the operational environment of the time. The effectiveness of the countermeasures against each type of threat is discussed. A software privacy transformation using an "infinite" key string

is presented. It is produced in real-time by two fast random-number generators; the key string is synchronized by an authenticated password.

[CARRJ 71A] Carroll, John M.; Martin, Robert; McHardy, Lorine; and Moravec, Hans; "Multi-dimensional Security Program for a Generalized Information Retrieval System," Proceedings of the Fall Joint Computer Conference, Vol. 39, 1971, p. 571-577, 5 refs.

This paper describes the functional password facility which is a part of the University of Western Ontario's Generalized Information Retrieval System (GIRS). In this password scheme, the passwords themselves contain the protection codes for data access.

[CARRJ 71B] Carroll, John M., and McLelland, P. M., "The Data Security Environment of Canadian Resource-sharing Systems, INFOR, Canadian Journal of Operational Research and Information Processing, 9:1, (March 1971), p. 58-67, 17 refs.

Several potential threats to the security of information in resource-sharing computer systems are reviewed together with countermeasures that may be used. Some general results of in-house attacks on an actual time-sharing system are reported along with conclusions drawn from a nationwide survey of the security provisions of Canadian computer utilities.

[CARRJ 73] Carroll, John M., and Reeves, Paul, "Security of Data Communications: A Realization of Piggyback Infiltration," INFOR, Canadian Journal of Operational Research and Information Processing, 11:3, (October 1973), p. 226-231, 2 refs.

The interception technique called "piggyback" infiltration is studied. Such a scheme was set up in order to better study the threat potentials involved. Possible defense measures are presented.

[COTTI 75] Cotton, Ira W., and Meissner, Paul, "Approaches to Controlling Personal Access to Computer Terminals," Proceedings of the 1975 Symposium Computer Networks: Trends and Applications, IEEE Computer Society, 1975, p. 32-39, 19 refs.

This is a state-of-the-art survey of the technology of personal identification and authentication in the computer environment. Threats and techniques for protection against these threats are discussed. Criteria for evaluating candidate personal

identification and authentication techniques are presented.

[DOWNP 77] Downey, Peter J., Multics Security Evaluation: Password and File Encryption Techniques, Electronic Systems Division (AFSC), Hanscom AFB, Mass., ESD-TR-74-193, Vol. III, in preparation.

[EVANA 74] Evans, Arthur Jr., and Kantrowitz, William, "A User Authentication Scheme Not Requiring Secrecy in the Computer," Communications of the ACM, 17:8, (August 1974), p. 437-442, 8 refs.

As an alternative to requiring that the password table remain hidden from would-be intruders, a scheme is proposed for transforming passwords via an essentially uninvertible function. These transformed passwords may then be observed by all users, along with the transformation function. This paper discusses issues surrounding selection of a suitable function. In addition, some human engineering problems relating to the scheme are discussed.

[FIPS 31] Jacobson, Robert V., William F. Brown and Peter S. Browne, Guidelines for Automatic Data Processing Physical Security and Risk Management, National Bureau of Standards, FIPS PUB 31, June 1974.

Provides guidelines to be used by Federal organizations in structuring physical security programs for their ADP facilities. Treats security analysis, natural disasters, supporting utilities, system reliability, procedural measures and controls, off-site facilities, contingency plans, security awareness and security audit.

[FIPS 39] Glossary for Computer Systems Security, National Bureau of Standards, FIPS PUB 39, February 1976.

This glossary was prepared in response to the need of Government agencies for a vocabulary of terminology related to the concepts of privacy and computer systems security.

[FIPS 41] Computer Security Guidelines for Implementing the Privacy Act of 1974, National Bureau of Standards, FIPS PUB 41, May 1975.

This publication provides guidelines for use by Federal ADP organizations in implementing the computer security safeguards necessary for compliance with Public Law 93-579, the Privacy Act of 1974. A wide variety of technical and related procedural safeguards are

described.

[FIPS 46] Data Encryption Standard, National Bureau of Standards, FIPS PUB 46, January 1977.

This publication provides a standard to be used by Federal organizations when these organizations specify that cryptographic protection is to be used for sensitive or valuable computer data. Ths standard specifies an encryption algorithm which is to be implemented in an electronic device for use in Federal ADP systems and networks. The algorithm uniquely defines the mathematical steps required to transform computer data into a cryptographic cipher. It also specifies the steps required to transform the cipher back to its original form.

[FIPS 48] Meissner, Paul, Guideline on Evaluation of Techniques for Automated Personal Identification, National Bureau of Standards, FIPS PUB 48, 1977 [in press].

This Federal guideline describes methods for verifying the identity of users seeking to gain access to computer systems or networks via terminals. Criteria are presented for evaluating the effectiveness of various personal identification techniques.

[FLETJ 73] Fletcher, John G., "Octopus Software Security," Proceedings of COMPCON 73, IEEE Computer Soceity, p. 61-62, 1 ref.

A fundamental design criteron of Lawrence Livermore Laboratory's Octopus computer network was secure network software. To better ensure such a secure system, the design relied primarily upon (1) processor hardware features which limit memory access and I/O activity of user programs being executed, (2) a system of secret combinations (passwords) for user identification, and (3) a file structure which provides for private, shared, and public files. Each of these features is discussed.

[FLETJ 75] Fletcher, J.G., Software Security in Networks, Lawrence Livermore Laboratory, University of California, 1975, 17p.

This report contains a more detailed treatment of Octopus network security.

[GASSM 75] Gasser, M., A Random Word Generator for Pronounceable Passwords, The MITRE Corporation, Bedford, Mass., AD-A017 676, November 1975, 183p., 3

refs.

Details of a random word generator designed to generate passwords for computer users are presented. The random word generator is a PL/I program designed to run on Honeywell's Multiplexed Information and Computer System (Multics). Goals and methods used by the random word generator are discussed; implementation details are given; and an analysis of the algorithm is presented.

[HAMMC 73] Hammer, Carl, "Electronic Data Systems Security," ADP Data Security and Privacy: Proceedings of the Conference on Secure Data Sharing, Naval Ship Research and Development Center, Bethesda, Md., Report 4130, August 1973, p. 188-197.

This article relates some of UNIVAC's activites in the computer security area. Current security enhancing features and capabilities of the EXEC 8 operating system are mentioned.

[HELDG 76] Held, Gilbert, "Locking Intruders Out of a Network," Executive Guide to Data Communications, McGraw-Hill Publications Co., New York, 1976.

Threats to passwords and applicable countermeasures are briefly discussed. Mention is made of some current and planned Multics protection mechanisms.

[HOFFL 69] Hoffman, Lance J., "Computers and Privacy: A Survey," Computing Surveys, 1:2, (June 1969), p. 85-103, 69 refs.

This paper is considered a "classic" in the field. It surveys the problems of access control and privacy in computer systems and reviews a number of suggested legal and administrative safeguards. A few promising computer science research problems in the field are outlined. A partially annotated bibliography is included.

[HOFFL 71] Hoffman, Lance J., "The Formulary Model for Flexible Privacy and Access Controls," Proceedings of the Fall Joint Computer Conference, Vol. 39, 1971, p. 587-601, 33 refs.

This paper presents an access control model which allows authorization decisions for data to be made at data access time, rather than solely at file creation time.

[IBM 74A] Data Security and Data Processing. Volume 1. Introduction and Overview, International Business

Machines Corporation, (G320-1370).

This is volume 1 of a six volume set of documents which report the findings of the IBM data security study conducted by the Massachusetts Institute of Technology, State of Illinois, the TRW Systems Group, and IBM's Federal Systems Center in Gaithersburg, Maryland. This volume discusses data security in general and briefly summarizes the study findings. It's intended audience is management.

[IBM 74B] Data Security and Data Processing. Volume 2. Study Summary, International Business Machines Corporation, (G320-1371.

This volume presents a brief summary of the study-site findings. It is primarily directed toward data processing management.

[IBM 74C] Data Security and Data Processing. Volume 3. Part 1 State of Illinois: Executive Overview, International Business Machines Corporation, (G320-1372).

The State of Illinois, with the assistance of IBM, has established the Secure Automated Facility Environment Project (Project SAFE) to develop reasonable safeguards for information systems. This volume addresses such questions as "Why bother with the privacy of information?" and "Does your organization have an information privacy problem?" A generalized information privacy action plan is presented.

[IBM 74D] Data Security and Data Processing. Volume 3. Part 2 Study Results: State of Illinois, International Business Machines Corporation, (G320-1373).

This volume presents an indepth treatment of the results of the State of Illinois' portion of the IBM data security study. Included is an overview of Project SAFE, an intensive treatment of the elements and economics of information privacy and security, recommended security practices, and a law school syllabus on information technology and the right to privacy.

[IBM 74E] Data Security and Data Processing. Volume 4. Study Results: Massachusetts Institute of Technology, International Business Machines Corporation, (G320-1394).

The MIT study was primarily concerned with the following: problem of access control, with emphasis on

authorization mechanisms; user needs for data security and the security awareness in the financial, medical, educational, and service bureau communities; how the study findings compared with the experience gathered by using RSS at MIT. This volume consists of 12 reports documenting the MIT study. Among the reports is an annotated bibliography of over 1000 citations.

[IBM 74F] Data Security and Data Processing. Volume 5. Study Results: TRW Systems, Inc., (G320-1375).

The TRW study was primarily concerned with the analysis of the nature of various vulnerabilities of computing systems, with the protection of computing systems against these vulnerabilities, and with current issues relating to the definition, application, accomplishment, and desirability of secure system certification.

[IBM 74G] Data Security and Data Processing. Volume 6. Evaluations and Installation Experiences: Resource Security System, International Business Machines Corporation, (G320-1376).

This volume summarizes the portion of the IBM study performed by the IBM Federal Systems Center. Also included are summaries of the MIT and TRW experiences with the IBM Resource Security System (RSS).

[IBM 76A] "IBM Introduces More Complete Security for MVs," Electronics News, (July 26, 1976), p. 16, 28.

This is an announcement of IBM's new data security system, Resource Access Control Facility (RACF). According to IBM, the system identifies and verifies users of the system, authorizes and logs access to protected disk files, and logs any detected unauthorized attempts to use the system.

[IBM 76B] OS/VS2 MVS Resource Access Control Facility (RACF) Command Language Reference, International Business Machines Corporation, (Program No. 5740-XXH9), August 1976, 78p.

[IBM 76C] OS/VS2 MVS Resource Access Control Facility (RACF) General Information Manual, International Business Machines Corporation, (Program No. 5740-XXH), August 1976, 48p.

[IBM 76D] "Automatic Password Generation for TSO," International Business Machines Corporation, 1976.

This is a small pamphlet which briefly describes the

highlights of the program.

[IBM 76E] TSO/Codes Update System: Program Description/Operations Manual, International Business Machines Corporation, (Program No. 5796-PFR), 1976, 34p.

TSO/Codes Update System is an automated TSO password generator and auditing system. This manual contains installation and operation information for that system.

[JARVJ 74] Jarvis, J.E. "Security in the Time-sharing Bureau," Proceedings of Computer Security 74, National Computing Centre Publications and IFIP Administrative Data Processing Group, 1974, p. 101-109.

Security features of Honeywell's Mark III Time-Sharing System, General Purpose Operating System (GCOS), and Multics are identified.

[JOHNS 74] Johnson, S.M., Certain Number Theoretic Questions in Access Control, Rand Corpotation, Report R-1494-NSF, January 1974.

This report examines the use of pseudorandom numbers as passwords. It reveals the vulnerabilities of many periodic password generation and distribution systems to simple, number-theoretic analysis. Strategies to reduce such vulnerabilities are proposed and analyzed.

[KARGP 74] Karger, Paul A. and Schell, Roger R., Multics Security Evaluation: Vulnerability Analysis, Electronic Systems Division (AFSC), Hanscom AFB, Mass., ESD-TR-74-193, Vol. II, June 1974, 156p, 33refs.

The Air Force conducted a security evaluation of Multics to determine its potential for use as a two-level (Secret/Top Secret) system in the Air Force Data Services Center. An overview of Multics Security controls and the results of penetration exercises on Multics systems are presented in this report.

[KAUFD 76] Kaufman, D., and Auerbach, K., "A Secure National System for Electronic Funds Transfer," Proceedings of the National Computer Conference, AFIPS Press, 1976, p. 129-138, 6 refs.

This paper presents guidelines for development of a secure national network for electronic funds transfer. Six security principles are given. The Personal Identification Number (PIN) is an integral part of EFTS. As the PIN is essentially a password, the related security principles are of great interest here.

[KENTS 76] Kent, Stephen T., "Encryption-Based Protection Protocols for Interactive User-Computer Communication," (Master's Thesis), Massachusetts Institute of Technology, Cambridge, Mass., AD-A026 911, May 1976, 122 p., 42 refs.

This thesis presents a set of protocols for protecting interactive user-computer communications over physically unsecured channels. Facilities are included for key distribution, two-way login authentication, resynchronization following channel disruption, and expedition of high priority messages.

[LIENB 74] Lientz, Bennet P. and Weiss, Ira R., On the Evaluation of Reliability and Security Measures in a Computer Network, Office of Naval Research, Arlington, Va., AD-A002 996, December 1974, 28p., 19 refs.

The relationship between networks and methods of enhancing reliability and security is considered, along with a discussion of past efforts. A methodology is developed for evaluating various measures in the context of a network.

[LUPTW 73] Lupton, William Lloyd, A Study of Computer Based Data Security Techniques, Naval Postgraduate School, Monterey, California, AD-765 677, 1973, 77p., 141 refs.

The results of a study which surveyed the various aspects of system security hardware, software, and procedural techniques are presented. In the discussion of software techniques, various password schemes are described.

[McCRR 73] McCraney, Ronn, "CDC's Current Procedures for Data Security," ADP Data Security and Privacy: Proceedings of the Conference on Secure Data Sharing, Naval Ship Research and Development Center, Bethesda, Md., Report 4130, August 1973, p. 199-200.

This very short paper mentions the design and implementation features of the hardware and software for privacy and security in CDC's 6000 and 7000 series and CYBER series of large-scale systems.

[MEISP 76] Meissner, Paul, Report of the 1976 Workshop on Estimation of Significant Advances in Computer Technology, National Bureau of Standards, (August 30-31, 1976), NBS-IR 76-1189, 70 p., [in press].

This is a summary of the results of a workshop held at the National Bureau of Standards. The workshop was intended to provide the Bureau with current scientific

and technical information on advances in computer technology which could significantly impact the Federal Government's knowledge and use of computer technology developments in relation to computer security and export administration.

[MUERJ 74] Muerle, John L.; Swonger, Claron W.; and Tona, Carmen J.; "EDP Security Through Positive Personal Identification," Proceedings of 1974 Carnahan and International Crime Countermeasures Conference, University of Kentucky, 1974, p. 246-253.

Although primarily a description of the FINGERSCAN system, this paper also contains a general discussion of various approaches to access control. Each approach is rated for reliability in normal operations, security against intentional compromise, fail-safe operation, user convenience, and response time.

[NEUMA 74] Neumann, A.J., A Guide to Networking Terminology, National Bureau of Standards, NBS Technical Note 803, March 1974, 29p.

This report contains a selected set of terms and definitions relating to computer networking.

[NEWS 76] "Twice-Scrambled Passwords Protect Customer Accounts," Minicomputer News, (October 7, 1976), p. 2.

Here is an example of "one-way" enciphering of passwords (PIN's) in a banking environment.

[NIELN 76] Nielsen, N. R.; Brandin, D. H.; Madden, J. D.; Ruder, B.; and Wallace, G. F.; Computer System Integrity Safeguards: System Integrity Maintenance, Stanford Research Institute, Menlo Park, California, SRI Project No. 4059, October 1976,.

This report presents the results of the first phase of the Computer System Integrity Research Program at SRI. This research focuses on the identification and analysis of the types of computer system integrity safeguards that would have been effective in preventing, detecting, or mitigating the effects of reported incidents of computer system integrity violations.

[NORTE 75] Northup, Ernest H., "Bank Cards Vs. the Underworld," Banking, 67:9, (September 1975), p. 66, 68, 70, 73.

This paper is a non-technical discussion of the basic elements of an EFT system, examining each component

from a security point of view.

[PARKD 73A] Parker, Donn B., Threats to Computer Systems, Lawrence Livermore Laboratory, UCRL-13574, March 1973, 118 p.

One-hundred and twenty nine cases of various types of computer-related losses, injuries, and damages are described, analyzed, or summarized in this report.

[PARKD 73B] Parker, Donn B.; Nycum, Susan; and Qura, S. Stephen; Computer Abuse, Stanford Research Institute, PK-231 320, November 1973, 181p.

This report is the second of a series of papers on computer abuse. (The first was [PARKD 73A], above.) It provides more generalized views of computer abuse -- technical, legal, and sociological perspectives.

[PARKD 76A] Parker, Donn B., "Computer Abuse Perpetrators and Vulnerabilities of Computer Systems," Proceedings of the National Computer Conference, AFIPS Press, Montvale, N.J., 1976, p. 65-73.

This is another of Donn Parker's interesting papers examining computer crime. In it he presents a profile of computer abuse perpetrators which was developed on the basis of interviews with offenders. Also described are computer systems' and user organizations' vulnerabilities that facilitated the crimes. Priorities for safeguards are deduced from the results of the study.

[PARKD 76B] Parker, Donn B., Crime by Computer, Charles Scribner's Sons, New York, 1976, 308p.

In this highly readable book, based on hundreds of investigated cases, Donn Parker discusses computer criminals, their motivations and crimes. Legal entanglements, violations of personal privacy, computer "intimidation," and the future of white-collar crime are also addressed.

[PETEB 67] Peters, Bernard, "Security Considerations in a Multi-programmed Computer System," Proceedings of the Spring Joint Computer Conference, Thompson Book Co., Washington, D.C., 1967, p. 283-286.

A set of principles for ensuring software security is presented. These principles were generalized from the development of a specific system which dealt with multi-levels of classified information. Among the principles discussed is the use of one-time passwords

to facilitate secure changes in security level by a user at a remote terminal.

[PETEH 67] Petersen, H.E., and Turn, R., "System Implications of Information Privacy," Proceedings of the Spring Joint Computer Conference, Thompson Book Co., Washington, D.C., 1967, p. 291-300, 14 refs.

This is an excellent discussion of the threat to information privacy in non-military information systems, applicable countermeasures, and system implications of providing privacy protection.

[POST 76] Peterson, Bill, "Convicted Computer Expert Seeks Role as Security Advisor," Washington Post, (August 4, 1976), p. B1.

[PURDG 74] Purdy, George B., "A High Security Log-in Procedure," Communications of the ACM, 17:8, (August 1974), p. 442-445, 8 refs.

A technique for one-way encipherment of passwords is presented.

[REEDS 74] Reed, Susan K., and Dennis K. Branstad, (editors), Controlled accessibility Workshop Report, National Bureau of Standards, NBS Technical Note 827, May 1974, 86p.

This is a report of the NBS/ACM Workshop on Controlled Accessibility held in December, 1972 at Rancho Santa Fe, California. Five working groups comprised the workshop: access controls, audit, EDP management controls, identification, and measurements. The report contains the introductory remarks outlining the purpose and goals of the Workshop, summaries of the discussions, and the conclusions reached. A list of participants is included.

[RICHM 73] Richardson, Mark H. and Potter, James V., Design of a Magnetic Card Modifiable Credential System Demonstration, Electronic Systems Division (AFSC), Hanscom Field, Mass., MCI-73-3, December 1973, 65p.

The design for a demonstration of a modifiable credential authentication scheme using magnetic cards and a read/write device for the cards is detailed. Unresolved issues are discussed.

[SHANC 49] Shannon, C.E., "Communication Theory of Secrecy Systems," Bell System Technical Journal, 28:4, (October 1949), p. 656-715.

Shannon developes and presents a mathematical theory of secrecy systems. The three main parts of the paper consider the following: the basic mathematical structure of secrecy systems, the problem of measuring how secure a system is against cryptanalysis ("theoretical secrecy"), and finally a section on "practical secrecy" -- methods for constructing systems which require a large amount of work to solve.

[TAYLA 75A] Taylor, Alan, "Darmstadt System Eliminates Check-Digit Loopholes," Computerworld, (September 17, 1975), p. 13.

[TAYLA 75B] Taylor, Alan, "Deeds Check-Digit Method Possibly Valuable DP Tool," Computerworld, (October 22, 1975), p. 11.

[TAYLA 76] Taylor, Alan, "Statistics Improving State of Art in 'Check-Digitry'," Computerworld, (February 23, 1976), p. 17.

[TESSE 76A] DAS: Data Access Security System: Technical Description, Tesseract Corporation, San Francisco, California, 1976, 11 p.

The Data Access Security system (DAS) is a commercial system offered as an improvement upon IBM's password protection support in existing operating systems. It is asserted by Tesseract that DAS I makes the password facility more generally usable and prevents the unauthorized disclosure of passwords. DAS II has been recently announced as a rewrite of IBM's password facility which allows increased functions and greater integrity of the system.

[TESSE 76B] DAS II: Product Announcement, Tesseract Corporation, San Francisco, California, October, 1976.

[TURNR 72] Turn, Rein, and Shapiro, Norman Z., "Privacy and Security in Databank Systems -- Measures of Effectiveness, Costs, and Protector-intruder Interactions," Proceedings of the Fall Joint Computer Conference, AFIPS Press, Montvale, N.J., 1972, p. 435-444, 26 refs.

A model of the personal information databank system is presented; the nature of the interactions of the databank security protector with potential intruders is explored; and the amount of security and costs associated with several classes of data security techniques are discussed.

[TURNR 74] Turn, Rein, Privacy Protection in Databanks:

Principles and Costs, The Rand Corporation, Santa Monica, California, AD-A023 406, September 1974, 21 p., 19 refs.

This paper was prepared for presentation at the Conference of Record Confidentiality and Criminal Justice Research Needs held in San Francisco on June 28, 1974. It singles out the more prominent protection principles and examines their cost implications in various types of databank systems.

[WEISC 69] Weissman, C., "Security Controls in the ADEPT-50 Time-sharing System," Proceedings of the Fall Joint Computer Conference, AFIPS Press, 1969, p. 119-133, 20 refs.

ADEPT-50 is a resource sharing system designed to handle sensitive information in classified government and military facilities. This paper describes the security controls implemented in the ADEPT-50 system.

[WILKM 75] Wilkes, M.V., Time Sharing Computer Systems, American Elsevier, New York, 1975.

This is the third edition of Wilkes' book, which was first published in 1968. It includes chapters on memory addressing and protection, scheduling and memory allocation, computer networks, and operational and managerial aspects of time-sharing.

[WINKS 74] Winkler, Stanley, and Danner, Lee, "Data Security in the Computer Communication Environment," Computer, (February 1974), p. 23-31, 7 refs.

This paper addresses some of the questions of data security in a computer communication environment, emphasizing the problems introduced by the merging of computers and communications. The functional aspects of data security (identification, authorization, controlled access, surveillance, and integrity) in such an environment are discussed.

[WOODH 77] Wood, Helen M., "On-line Password Techniques," Proceedings of Trends and Applications: 1977 - Computer Security and Integrity Symposium, IEEE Computer Society, May 1977.

This paper classifies the features of on-line password schemes according to password selection/assignment technique, lifetime, and content. Some advantages and disadvantages of implementations of these features are discussed and illustrative examples are given.

* U. S. GOVERNMENT PRINTING OFFICE: 1977--260-584/115

NBS-114A (REV. 7-73)

U.S. DEPT. OF COMM. BIBLIOGRAPHIC DATA SHEET	1. PUBLICATION OR REPORT NO. NBS SP 500-9	2. Gov't Accession No.	3. Recipient's Accession No.

4. TITLE AND SUBTITLE

The Use of Passwords for Controlled Access to Computer Resources

5. Publication Date May 1977

6. Performing Organization Code

7. AUTHOR(S) Helen M. Wood

8. Performing Organ. Report No.

9. PERFORMING ORGANIZATION NAME AND ADDRESS

NATIONAL BUREAU OF STANDARDS
DEPARTMENT OF COMMERCE
WASHINGTON, D.C. 20234

10. Project/Task/Work Unit No. 6501104

11. Contract/Grant No.

12. Sponsoring Organization Name and Complete Address *(Street, City, State, ZIP)*

13. Type of Report & Period Covered Interim

14. Sponsoring Agency Code

15. SUPPLEMENTARY NOTES

Library of Congress Catalog Card Number: 77-5558

16. ABSTRACT *(A 200-word or less factual summary of most significant information. If document includes a significant bibliography or literature survey, mention it here.)*

This paper considers the generation of passwords and their effective application to the problem of controlling access to computer resources. After describing the need for and uses of passwords, password schemes are categorized according to selection technique, lifetime, physical characteristics, and information content. Password protection, both in storage and transmission, is dealt with in the next section, followed by brief sections on current implementations and cost considerations. A glossary and an annotated bibliography of all referenced material are included.

17. KEY WORDS *(six to twelve entries; alphabetical order; capitalize only the first letter of the first key word unless a proper name; separated by semicolons)*

Computer networking; computer security; controlled access; identification; passwords; personal authentication

18. AVAILABILITY

[X] Unlimited

[ ] For Official Distribution. Do Not Release to NTIS

[X] Order From Sup. of Doc., U.S. Government Printing Office Washington, D.C. 20402, SD Cat. No. C13.10:500-9

[ ] Order From National Technical Information Service (NTIS) Springfield, Virginia 22151

19. SECURITY CLASS (THIS REPORT)	21. NO. OF PAGES
UNCLASSIFIED	59
20. SECURITY CLASS (THIS PAGE)	**22. Price** $2.00
UNCLASSIFIED	

USCOMM-DC 29042-P74

ANNOUNCEMENT OF NEW PUBLICATIONS ON COMPUTER SCIENCE & TECHNOLOGY

Superintendent of Documents,
Government Printing Office,
Washington, D. C. 20402

Dear Sir:

Please add my name to the announcement list of new publications to be issued in the series: National Bureau of Standards Special Publication 500-.

Name _____

Company _____

Address _____

City _____ State _____ Zip Code _____

(Notification key N-503)